UNITED STATES DISTRICT COURT
DISTRICT OF DELAWARE

IN RE GOOGLE INC. COOKIE PLACEMENT CONSUMER PRIVACY LITIGATION	Case No. 12-MD-2358 (SLR)
This Document Relates to: **All Actions**	

PLAINTIFFS' BRIEF IN OPPOSITION TO
DEFENDANT POINTROLL, INC.'S MOTION TO DISMISS

KEEFE BARTELS, LLC
Stephen G. Grygiel (Del Bar No. 4944)
John E. Keefe, Jr.
Jennifer L. Harwood
170 Monmouth St.
Red Bank, NJ 07701
Tel: 732-224-9400
sgrygiel@keefebartels.com

Executive Committee Member

STRANGE & CARPENTER
Brian Russell Strange
Keith Butler
David Holop
12100 Wilshire Boulevard, Suite 1900
Los Angeles, CA 90025
Tel: 310-207-5055
lacounsel@earthlink.net

Executive Committee Member

BARTIMUS, FRICKLETON, ROBERTSON & GORNY, P.C.
James P. Frickleton
Mary D. Winter
Stephen M. Gorny
Edward D. Robertston, Jr.
11150 Overbrook Road, Suite 200
Leawood, KS 66211
Tel: 913-266-2300
jimf@bflawfirm.com

Executive Committee Member

STEWARTS LAW US LLP
Ralph N. Sianni (Del Bar No. 4151)
Michele S. Carino (Del Bar No. 5576)
Lydia E. York (Del Bar No. 5584)
I.M. Pei Building
1105 North Market Street, Suite 2000
Wilmington, DE 19801
Tel: 302-298-1200
rsianni@stewartslaw.com

Plaintiffs' Steering Committee Member and Liaison Counsel

[Additional Counsel on Signature Page]

Dated: March 29, 2013

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

OTHER AUTHORITIES

RULES

I. NATURE AND STAGE OF THE PROCEEDINGS

Plaintiffs filed their first Consolidated Amended Compliant ("CAC") in this MDL on December 19, 2012. Defendant PointRoll filed a Motion to Dismiss under Fed. R. Civ. P. 12(b)(6). Plaintiffs' opposition is below.

II. SUMMARY OF ARGUMENT

1. PointRoll's Motion is based on factual issues the CAC and its attendant inferences contradict, requiring denial of that motion and discovery.

2. Plaintiffs have pled constitutional and statutory standing. The CAC shows the actual value of Personal Information that PointRoll illicitly took. PointRoll's invasion of Plaintiffs' statutorily protected rights is itself injury in fact.

III. STATEMENT OF FACTS

Plaintiffs' factual allegations are deemed true on this dismissal motion. *See Phillips v. Cnty. of Allegheny*, 515 F.3d 224, 233 (3d Cir. 2008). Plaintiffs' factual allegations contradict PointRoll's misleading portrayal of its use of an undisclosed code and accompanying invisible iframe that tricked users' browsers into accepting PointRoll's nine cookies, including PointRoll's tracking cookie. CAC ¶¶ 130-134.

A leading provider of online advertising, PointRoll claims to "[p]ower[] 55% of all rich media campaigns online" and "serve over 450 billion impressions for more than two-thirds of the Fortune 500 brands." CAC ¶ 20. Trying to increase its business, PointRoll "joined with Google" to offer advertisements, creative services, and "**targeting and extensive tracking** and measurement capabilities on a significantly expanded number of websites." *Id.* ¶ 22. PointRoll's "targeting and extensive tracking" led PointRoll, through its affiliation with Apple, to begin secretly disabling users' Safari browser default "do not track" settings (*id.* ¶¶ 70–71) to intercept and gain unauthorized access to users' information. *Id.* ¶ 127. When a user navigates

to a webpage containing PointRoll ads, the browser sends a GET request to that webpage to send all information for that webpage back to the user's browser for display on the user's device. *Id.* ¶ 128. The webpage sends a GET request to PointRoll to display the relevant PointRoll ads. *Id.* ¶¶ 129–30. Without any user action, the PointRoll server responds to the GET request with code that includes an invisible form that is automatically submitted back to PointRoll's server. *Id.* ¶ 130. The invisible form and its accompanying code trick the user's browser into requesting cookies without the user's permission or knowledge, evading Safari's default cookie-blocking features and permitting PointRoll secretly to store nine cookies on the user's device. *Id.* ¶¶ 131-33.

Plaintiffs allege on information and belief that PointRoll's "PRID" cookie was created to track persons across all websites that PointRoll serves with ad content. *Id.* ¶ 134. PointRoll's then-CEO Rob Gatto essentially confirmed PointRoll's surreptitious cookie placement in a February 17, 2012 blog post. *Id.* ¶¶ 136-38. Confirming that PointRoll adopted a known hacking technique developed in 2010 by developer Anant Garg (*id.)*, Mr. Gatto stated: "PointRoll does not currently employ the Safari technique outlined in [a February 17, 2012 Wall Street Journal] article.[1] PointRoll conducted a limited test within the Safari browser to determine the effectiveness of our mobile ads." *Id.* ¶ 136. Stanford's Jonathan Mayer concluded that PointRoll's "cookie blocking circumvention was intentional."[2] *Id.* ¶¶ 75, 138. Mr. Mayer damningly compared the code PointRoll used to circumvent the Safari default settings to Mr. Garg's code. *Id.* ¶ 138. PointRoll used existing code from Mr. Garg's article. PointRoll's code was "structured in the same way" as Mr. Garg's code. Both used the same "variable sessionForm and the handler function submitSessionForm." Both possessed "the same attributes,

[1] *See* Google Request for Judicial Notice, Ex. 4.
[2] *Id.*

attribute ordering, and coding style." *Id.* Convincingly demonstrating PointRoll's intentional deception, Mr. Garg's code and PointRoll's code both contained "the same bug." *Id.*

Plaintiffs need only "'allege facts suggestive of [the proscribed conduct]'" *Phillips*, 515 F.3d at 233 (quoting *Bell Atlantic Co. v. Twombly*, 550 U.S. 544, 563 n.8 (2007)). Mr. Mayer's analysis of PointRoll's intentional trickery (CAC ¶ 138), and PointRoll's Mr. Gatto's cryptic "we're not doing it anymore" explanation that nowhere mentioned user knowledge, user consent, or technological accident (CAC ¶¶ 136, 139-145) at a minimum "'raise a reasonable expectation that discovery will reveal evidence of '" the elements of Plaintiffs' claims. *Phillips,* 515 F. 3d at 234 (quoting *Twombly*, 550 U. S. at 556)). Plaintiffs here do not even need the benefit of inferences, to which they are entitled, that PointRoll secretly tracked users. PointRoll admits it. CAC ¶¶ 136 ("PointRoll conducted a limited test…").

IV. STANDING

PointRoll's relegation of its perfunctory Article III standing argument to a few pages at the end of its brief underscores that argument's fatal weakness. As now-Justice Alito said: "Injury-in-fact is not Mount Everest." *Danvers Motor Co. Inc. v. Ford Motor Co., Inc.*, 432 F. 3d 286, 294 (3d Cir. 2005) (citing *Bowman v. Wilson,* 672 F.2d 1145, 1151 (3d Cir. 1982)). PointRoll ignores the long-established rule that at this stage Plaintiffs need only generally allege (*see Lujan v. Defenders of Wildlife,* 504 U.S. 555, 561 (1992)) "an identifiable trifle" of harm. *U.S. v. Students Challenging Reg. Agency Procedures ("SCRAP"),* 412 U.S. 669, 689 n.14 (1973). *See also Bowman*, 672 F.2d at 1151 ("contours of the injury-in-fact requirement…are very generous" and "'identifiable trifle' of alleged injury" suffices (quoting *U.S. v. SCRAP*, 412 U.S. at 686-90, 689 n. 14)). PointRoll nowhere explains how Plaintiffs' allegations of PointRoll's wrongful gathering of the contents of Plaintiffs' electronic communications through an invisible code permitting secretly placed tracking cookies (*see* CAC ¶¶ 1-4, 127-145, 198-

212) and unauthorized secret access to Plaintiffs' electronic communications (*see* CAC, ¶¶ 213-219, 220-227) are not an "identifiable trifle" of personal harm. PointRoll must have thought Plaintiffs and other users would experience harm, or PointRoll would not have concealed its serial technological tricks (CAC ¶¶ 127-135) to defeat Safari. CAC ¶¶ 139-143. PointRoll's conclusory argument that Plaintiffs do not allege *enough* harm (D. Br. 19) ignores settled law. Harm much less than PointRoll's invasion of Plaintiffs' statutorily protected rights, suffices. *See U.S. v. SCRAP*, 412 U.S. at 689 n.14 (rejecting limitation of standing to those "'significantly' affected" by agency action: "We have allowed important interests to be vindicated by plaintiffs with no more at stake…than a fraction of a vote,…a $5 fine and costs,…and a $1.50 poll tax").

PointRoll argues that Plaintiffs lack statutory standing under the Wiretap Act (Count I), Stored Communication Act (Count II) , and Computer Fraud and Abuse Act (Count III) because those statutes "do not expressly grant rights against or with respect to Internet cookies, and have not previously been construed to protect Internet users from desired or undesired cookies." That is like a burglar saying the burglary statute does not specifically prohibit theft using a 9.5" yellow crowbar. PointRoll cites no case, and Plaintiffs are aware of none, holding any of those statutes unavailable to plaintiffs whose claims are based on cookie-facilitated unlawful interceptions or unauthorized access. PointRoll argues *Alston v. Countrywide Fin. Corp.*, 585 F.3d 753 (3d Cir. 2009), "should not control the statutes at issue here." D. Br. 19, 20. PointRoll ignores *Alston's* clear affirmation (*id.* at 762-63) that statutory standing exists where, as here, Plaintiffs allege Defendant violated Plaintiffs' own rights under a statute – even if that invasion of Plaintiffs' statutory rights caused Plaintiffs no financial or other harm. *See Warth v. Seldin*, 422 U.S. 490, 500 (1975); *Lujan*, 504 U.S. at 578.

PointRoll's argument that Plaintiffs do not allege "factual predicates" for their statutory claims ignores Mr Gatto's admission (CAC ¶¶ 136,137), Mr. Mayer's analysis (*id.* ¶ 138), the inferences from PointRoll's conspicuous silence on secrecy and consent points (*id.* ¶¶ 139-144) and many other facts. Pointroll's wished-for statutory standing requirement of "statutory standing plus additional injury"" (D. Br. 19) finds support nowhere in the cases or the Constitution. PointRoll cites *Summers v. Earth Island Inst.,* 555 U.S. 488, 497 (2009),[3] and *Raines v. Byrd,* 521 U.S. 811, 820 n.3 (1997)[4] for the settled separation-of-powers principle, not at issue here, that Congress cannot legislatively remove Article III's baseline requirement of injury-in-fact and confer standing on persons who have suffered no injury or have not been deprived of statutory rights that they would seek to vindicate. PointRoll's footnote argument (D. Br. 19 n.27), citing *Joint Stock Soc'y v. UDV N Am., Inc.,* 266 F.3d 164, 176 (3d Cir. 2001), and *Doe v. Nat'l Bd. Of Med. Exam.,* 199 F.3d 146, 153 (3d Cir. 1999), wishes away Supreme Court precedent such as *Warth* and *Lujan* holding that the Plaintiffs' properly alleged violations of their own statutory rights *is* injury-in-fact, redressable by statutory damages. PointRoll's separation of its invasion of the Plaintiffs' protected statutory rights from injury-in-fact (standing question "is

[3] *Summers*, an organizational standing case, involved an environmental group's effort to compel the U.S. Forest Service to apply certain regulations. Among other differences from our case, *Summers's* plaintiffs asserted only vague intentions to visit the supposedly threatened sites at some unspecified future date. *See Summers,* 555 U.S. at 496. Such allegations of only potential future harm differ dispositively from our Plaintiffs' personalized, concrete and particularized already-incurred injuries from PointRoll secretly hacking around the Safari browsers' cookie-blocking default setting to get Plaintiffs' information without permission or authorization. CAC ¶¶ 1-4, 127-145.

[4] *Raines* involved four Senators and two Congressmen challenging the constitutionality of the Line Item veto. Applying an "especially rigorous" "standing inquiry" (*Raines*, 521 U.S. at 820-21) to this "legislative standing question" of first impression (*id.* at 820), because it required a decision that another governmental branch had acted unconstitutionally, *Raines* differs dramatically from our case. *Raines's* six legislators needed to fit themselves into the very tight box of a single case (*Coleman v. Miller,* 307 U.S. 433 (1939)) and failed. Plaintiffs here need only generally allege injury-in-fact that is no more than an "identifiable trifle."

not whether PointRoll violated a statutory right, but whether the accused actions caused a redressable injury-in-fact" (D. Br. 19 n.27)) would require rewriting *Warth, Lujan* and many other cases. *In re Google, Inc. Privacy Policy Litig.*, No. C12-01382, 2012 WL 6738343, at * 5-6 (N.D. Cal. Dec. 28, 2012) (D. Br. 18), confirms Plaintiff's statutory standing.[5] Nor do *Joint Stock Soc'y. v. UDV N. Am. Inc.*, 266 F.3d 164, 177 (3d Cir. 2001),[6] and *Doe v. Nat'l. Bd. Med. Exam'rs.*, 199 F. 3d 146, 153 (3d Cir. 1999)[7] (D. Br. 19, n. 27). Finally, PointRoll's cites to *LaCourt v. Specific Media*, No. SACV 10-1256-GW (JCGX), 2011 WL 1661532, *4-5 (C.D. Cal. April 28, 2011), *In re JetBlue Airways Corp. Privacy Litig.*, 379 F. Supp. 2d 299, 327 (E.D.N.Y 2005), *Dwyer v. Am. Express Co.*, 273 Ill. App. 3d 743 (Ill. App. Ct. 1995), *Reilly v. Ceridian Corp.*, 664 F.3d 38, 42 (3d Cir. 2011) and *Allison v. Aetna*, No. 09-2560, 2010 WL 3719243 (E.D. Pa. March 9, 2010) (D. Br. 20) get PointRoll nowhere.[8]

---

[5] In *Google*, the Plaintiffs failed "to allege injury in fact to themselves." 2012 WL 6738343 at *4. Plaintiffs in our case allege injury to *themselves. See, e.g.*, CAC ¶¶ 1-4, 199-201, 205-208, 216-219, 224-227. The *Google* court said plaintiffs' Wiretap Act claim may have provided standing, but it only alleged interception by Google, which already possessed the supposedly intercepted information and ran afoul of the Act's "device" exception for "a provider's own equipment in the ordinary course of business." *Google*, 2012 WL 6738343, * 5-6.

[6] Addressing standing at the summary judgment, not pleadings, stage, and endorsing the "identifiable trifle" test (*Joint Stock*, 266 F.3d at 177) (citing *U.S. v. SCRAP*, 412 U.S. at 689 n.14), the court found no standing because plaintiffs, claiming false advertising injury, had "not even begun offering their product for sale in the United States." *Joint Stock*, 266 F.3d at 176. This case would be analogous only if Plaintiffs merely *considered* using Safari browsers on the chance they *might* some day visit websites.

[7] Unlike our case, *Doe* was *not* a pleadings case, but a Preliminary Injunction case, so, unlike our case, "mere allegations will not support standing." *Doe*, 199 F. 3d at 152.

[8] *Specific Media's* plaintiffs, unlike Plaintiffs here, did not allege they were personally affected by Defendant's practices. 2011 WL 1661532 at *4-5. Even so the *Specific Media* court did not categorically find it "impossible for Plaintiffs to allege some property interest that was compromised by Defendant's alleged practices. The problem is, at this point, they have not done so." *Id.* at *4. *Specific Media* recognized "the viability in the abstract of … concepts" showing PII's value. *Id.* Unlike in *Specific Media*, Plaintiffs have alleged not "quasi-philosophical"

V. LEGAL ARGUMENTS

A. COUNT I – THE COMPLAINT STATES A CLAIM UNDER THE ELECTRONIC COMMUNICATIONS PRIVACY ACT ("ECPA")

"The paramount objective of the Wiretap Act is to protect effectively the privacy of communications." *In re Pharmatrak, Inc.*, 329 F.3d 9, 18 (1st Cir. 2003). Enacted in 1986, the "ECPA amended the Federal Wiretap Act[9] by extending to data and electronic transmissions the same protection already afforded to oral and wire communications."[10] *Id.*

Plaintiffs allege a valid Wiretap Act claim, showing: (1) PointRoll intercepted the "contents" of communications between Plaintiffs and first-party websites by designing code that

---

debating points about PII, but have specifically alleged dollar values the industry ascribes to such data. *See* CAC ¶¶ 49-67.

JetBlue was a merits opinion, entailing a materially different inquiry from that for a 12(b)(1) standing question. *See, e.g.*, *Warth*, 422 U.S. at 500 (standing "in no way depends on the merits). *JetBlue's* plaintiffs did not allege the commercial value of PII with attendant specific dollars for different categories of PII.

Reilly confirms Plaintiffs' point: general factual allegations of injury suffice for standing. Unlike our case, *Reilly*, a data breach case, included no allegations of misuse of the compromised data and no allegations showing any imminent future misuse. *Reilly*, 664 F.3d at 44. Plaintiffs here allege that PointRoll *already* illegally captured Plaintiffs' electronic communications for PointRoll's own economic benefit. *Allison* is an inapposite data breach case akin to *Reilly*, involving claims of potential future harm. *Allison's* plaintiff had not alleged that the "security breach of Defendant's online job application database" (2010 WL 3719243 at *1) had *any* effect on the plaintiff at all.

Dwyer (an Illinois state court case) involved the very different case of cardholder plaintiffs contending that information they had voluntarily given to American Express produced a surfeit of unwanted solicitations and other mail. *Dwyer*, 273 Ill. App. 3d at 743-44. Plaintiffs here did not voluntarily provide information to PointRoll.

[9] PointRoll characterizes the Wiretap Act as "primarily a criminal statute." D. Br. 11. But 18 U.S.C. § 2520 expressly creates a civil cause of action.

[10] "…[L]egislation which protects electronic communications from interceptions…should be comprehensive, and ***not limited to particular types or techniques of communicating***….Any attempt to…protect only those technologies which exist in the marketplace today…is destined to be outmoded within a few years….what is being protected is ***the sanctity and privacy of the communication***. We ***should not attempt to discriminate for or against certain methods of communication***…." 132 Cong. Rec. H4039-01 (1986) 1986 WL 776505 (comments from Representative Kastenmeier) (emphasis added).

tricked Plaintiffs' browsers' "do not track settings" (CAC ¶¶ 127-135); (2) PointRoll was not a party to the communications it intercepted, as its need to trick Plaintiffs' browsers shows; (3) neither Plaintiffs nor the websites consented to PointRoll's clandestine interceptions (CAC ¶¶ 139-141); and (4) PointRoll used "devices" to intercept Plaintiffs' communications (CAC ¶¶ 127, 130-135). Because Plaintiffs have pleaded facts showing an unlawful interception, they may also plead use and disclosure claims under 18 U.S.C. § 2511(1)(c)-(d).

1. PointRoll Intercepted[11] the "Content" of Communications

The Wiretap Act defines "contents" to mean "information concerning the substance, purport, or meaning of" a communication. 18 U.S.C. § 2510(8). PointRoll factually and wrongly contends it intercepted mere "transactional information" in an effort to invoke inapplicable precedent saying such information is not "content." PointRoll intercepted transactional information ***and*** "contents." *See, e.g.,* CAC ¶ 145.

PointRoll circumvented Plaintiffs' browsers' settings to intercept: (1) the specific URLs Plaintiffs requested from first-party websites, which identified "specific items, such as websites, videos, pictures, or articles" that each Plaintiff chose to view; and, (2) "information that Class Members exchanged with first-party websites during the course of filling out forms or conducting searches." Defendant intercepted "not just the fact of a request, but the exact request itself, which, because it includes URL information, is substantive." CAC ¶ 205-207.

Intercepting URLs constitutes interception of "content." *See U.S. v. Forrester*, 512 F.3d 500, 510 n.6 (9th Cir. 2008) (URL constitutes "content" because URL "identifies a particular document within a website that person views and reveals much more information about a

[11] Plaintiffs have satisfied the "interception" element. *See U.S. v. Szymuskiewicz,* 622 F.3d 701, 706-707 (7th Cir. 2010); *see also In re Pharmatrak,* 329 F.3d at 21-22; *In re DoubleClick,* 154 F. Supp. 2d 497, 514 (S.D. N.Y. 2001) (DoubleClick conceded that its conduct there violated 18 U.S.C. § 2511(1)(a)).

person's Internet activity"); *In re Application of the United States for an Order Authorizing the Use of a Pen Register and Trap*, 396 F. Supp. 2d 45, 49 (D. Mass. 2005) (URL constitutes "content" because "substance" and "meaning" of communication is user's search for information on particular topic.)[12] Even the *Pen Register* case upon which PointRoll relies distinguishes between online transactional data (such as an IP address) and contents (such as a URL). *See In re Application of the U.S. for an Order Authorizing the Use of a Pen Register and Trap & Trace Device on E-Mail Account*, 416 F. Supp. 2d 13, 18 n.7 (D.D.C. 2006).[13] The Court concluded that a pen register should "exclude all information relating the subject line and body" of an email communication lest it be transformed into an "electronic interception device." *Id.* at 17-18. The same analysis applies to URLs.[14]

Finally, Defendant overstates Rule 8's requirements, arguing that Plaintiffs were required to plead the identity of specific websites they visited. A complaint "does not need ***detailed*** factual allegations." *See Twombly*, 550 U.S. at 555. (emphasis added). It only requires facts that "raise a right to relief above a speculative level." *Id. See also Phillips*, 515 F.3d at 237

---

[12] For example, "[a] GET request for www.helpfordrunks.com with information about where to find AA meetings in Wilmington," tells anyone intercepting that communication much about the user. CAC ¶ 207.

[13] Contrary to PointRoll's discussion of *Pen Register*, 416 F. Supp. 2d at 18, n.7, that court did not determine that URLs were transactional and not content. PointRoll furtively slipped "URLs" into the list of transactional items (IP addresses, date and time of communication, etc…) the court *did* reference (D. Br. 12).

[14] In *Brown v. Waddell*, 50 F.3d 285 (4th Cir. 1995), police obtained "pager clones" which intercepted additional number codes, one of which indicated that a caller was "en route." *Id*. at 287-88. The Fourth Circuit held that these additional numbers were "contents" under the Wiretap Act. *Id*. at 294. If numbers on a pager are "content," so too are the actual words and numbers in a URL string.

Smith v. Trusted Universal Standards in Elec. Transactions, Inc., No. 09-4567 (RBK/KMW), 2010 WL 1799456, at *11 (D.N.J. May 4, 2010), is also inapposite. *Smith* involved a *pro se* litigant who failed to allege that that any of his communications were intercepted, whereas Plaintiffs have alleged such.

(plaintiffs' failure to allege where shootings occurred offered no basis for dismissal, noting "preliminary pleading stage," and "reasonable" inferences to which plaintiffs were entitled). The CAC alleges facts that Plaintiffs visited websites with third-party advertisements from PointRoll. CAC ¶¶ 10-14. Plaintiffs further allege that upon visiting those sites, PointRoll secretly disabled their web browsers' "do not track" settings with code that allowed PointRoll to place third-party tracking cookies that intercepted Plaintiffs' communications with other websites. CAC ¶¶ 127-145. These facts have enough "heft" for plausibility. *Twombly*, 550 U.S. at 557. Rule 8(a)(2) does not require Plaintiffs to plead details or specific evidence. *See Twombly*, 550 U.S. at 555; *Phillips*, 515 F.3d at 234 (explication of *Twombly* "can be reduced to this proposition: Rule 8(a)(2) has it right." (citation omitted)).

2. PointRoll Was Not a Party to the Communication; It May Not Manufacture a Statutory Exception Through Its Own Illegal Conduct

PointRoll tries to invoke a Wiretap Act exception (18 U.S.C. § 2511(2)(d)) that protects the communication's intended recipient. *See In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1062 (N.D. Cal. 2012). The CAC, however, pleads facts showing PointRoll was not an intended party to Plaintiffs' communications with first-party websites, and Plaintiffs' browsers were specifically configured to ***prohibit*** PointRoll from becoming a party. CAC ¶¶ 69-73, 180, 199. PointRoll only accessed Plaintiffs' communications by tricking Plaintiffs' web browsers into providing their online communications to PointRoll. CAC ¶¶ 127-145, 183-188, 201-203. PointRoll cannot manufacture a statutory exception to the Wiretap Act through its own misconduct. *See In re iPhone Application Litig.*, 844 F. Supp. 2d at 1062. (where plaintiffs had

not intended any communication, a Wiretap Act defendant like Apple "cannot manufacture a statutory exception through its own accused conduct").[15]

3. PointRoll Lacked Consent from a Party to the Communication

Stated separately in 18 U.S.C. § 2511(2)(d), the consent exception is an affirmative defense that PointRoll must establish. *See Pharmatrak,* 329 F.3d at 19. It is not appropriately the subject of this motion. *See, e.g., Scott v. Kuhlman,* 746 F.2d 1377, 1378 (9th Cir. 1984) (citing Wright & Miller, *Federal Practice and Procedure,* § 1277 at 328-30) (affirmative defenses may not be raised in a motion to dismiss unless there are no disputed issues of fact). PointRoll's legally baseless argument is that Plaintiffs' claims fail because, according to PointRoll, Plaintiffs' Complaint does not disprove PointRoll's fact-intensive affirmative defense. *See Valentine v. Wideopen West Finance,* No. 09 C 7653, 2012 WL 6642375, at *5 (N.D. Ill. Dec. 20, 2012) (plaintiffs need not anticipate affirmative defense of consent; contested consent issue no basis for dismissal and required discovery at pleadings stage).

Even if PointRoll could hint at some "consent," consent "should not be casually inferred." *In re Pharmatrak,* 329 F.3d at 20. Emphasizing consent's fact-intensive nature, courts use a two-part inquiry: First, a court must determine the "dimensions of consent." *Id.* at 19. Then, it must "ascertain whether the interception exceeded those boundaries." *Id.* PointRoll erroneously infers unlimited consent from PointRoll's hidden receipt of a GET request for an ad. However, neither Plaintiffs, nor the websites they visited, consented to PointRoll tricking Plaintiffs' browsers into accepting tracking technologies the browser was configured to block.

[15] *Ideal Aerosmith v. Acutronic USA, Inc.*, C.A. No. 07-1029, 2007 WL 4394447 (E.D. Pa. Dec. 13, 2007) is also not analogous. There the plaintiff's Wiretap Act claim was based upon emails sent ***directly*** to a server owned by the defendant, a successor in interest who had purchased a bankrupt company's assets. Here, Plaintiffs' browsers were configured to *prohibit* PointRoll from gaining access to plaintiffs' communications with other websites. Plaintiffs never intended PointRoll to obtain the substance of communications with these websites.

Plaintiffs' browser settings vitiate user consent. Websites, after learning of Google's identical conduct, stated: we "were not aware of this behavior," "would never condone it," and "we don't support this activity." CAC ¶ 126. PointRoll has provided no evidence ***any*** website consented to its conduct, let alone that ***all*** of them consented. Plaintiffs, thus, are not required to plead facts showing a tortious or criminal purpose. 18 U.S.C. § 2511(2)(d).[16]

Finally, PointRoll's reliance on *In re DoubleClick Inc. Privacy Litig.*, 154 F. Supp. 2d 497 (S.D.N.Y.), is misplaced. *See* 154 F. Supp. 2d at 504-05. That court based its decision in part on a fact contrary to the facts in Plaintiffs' CAC:

> DoubleClick will not collect information from any user who takes simple steps to prevent DoubleClick's tracking…users can easily…prevent DoubleClick from collecting information from them. They may do this in two ways:…(2) ***configuring their browsers to block any cookies from being deposited.***

Id. (emphasis added). The CAC alleges that PointRoll, secretly using Mr. Garg's code, was doing exactly what the Southern District of New York was led to believe was not involved in *In re DoubleClick* – collecting information from users who took "simple steps to prevent…tracking" such as "configuring their browsers to block any cookies from being deposited." *In re DoubleClick* does not bar Plaintiffs' Wiretap Act claim.

4. PointRoll Used "Devices"[17] to Intercept Plaintiffs' Communications.

The Wiretap Act defines an "electronic…device" broadly as "any device or apparatus which can be used to intercept a[n]…electronic communication." 18 U.S.C. § 2510(5). The

[16] PointRoll's brief misconstrues 18 U.S.C. § 2511 (2)(d). Pleading tortious or criminal intent is only necessary for establishing an exception to an affirmative defense; it is not an element of the claim. *See Caro v. Weintraub*, 618 F.3d 94, 101 (2d Cir. 2010) ("The language and history of the Wiretap Act indicate that Congress authored the exception to the one-party consent rule to prevent abuses stemming from use of the recording not the mere act of recording").

[17] PointRoll's insinuation that a "device" can only be something like an "alligator clip" reflects an outdated view of the Wiretap Act inconsistent with the purposes underlying ECPA (*See* fn. 10, *supra*) and would eviscerate the Act in the digital age. *See, e.g. Byrd v. Shannon*, 2013 WL 870210, at * 2 (3d Cir. Mar. 11, 2013) (court's task "to give effect to the will of Congress").

CAC alleges PointRoll's use of special unblocking software codes that allowed PointRoll to plant third-party cookies that intercepted the Plaintiffs' electronic communications with first-party websites. CAC ¶¶ 201-02. PointRoll placed that code and cookies via computers and servers. PointRoll employed these electronic devices to intercept Plaintiffs' communications. As a matter of law, webservers and computers are "devices." *See Szymuszkiewicz*, 622 F.3d at 707; *In re Pharmatrak,* 329 F.3d at 18-19. No court has ever found that servers, browsers, cookies, or any schemes using them to intercept communications are not "devices." PointRoll's co-defendant did not even bother to raise this argument and PointRoll offers no support for it.

5. Allegations Showing Improper Interception Authorize the Pleading of Use and Disclosure Allegations.

PointRoll's use and disclosure argument is premised upon its fallacious factual claim that it was party to, or had consent to track, Plaintiffs' communications. Because Plaintiffs have pled facts that must be taken as true and establish unlawful interceptions, Plaintiffs can assert use and disclosure allegations under 18 U.S.C.§ 2511(1)(c)-(d).

6. Conclusion: Plaintiffs Have Stated Valid Wiretap Act Claims

Faced with Plaintiffs' entirely plausible Wiretap Act claim, PointRoll retreats to a grossly overstated, policy-based slippery slope argument, that Plaintiffs' claims, if successful, would "broadly and unpredictably impact the internet."

Congress' application of the Wiretap Act to telephone technologies did not broadly and unpredictably affect the telecommunications industry. Rather, the Wiretap Act held responsible those who used those technologies surreptitiously in ways violating the Act. Similarly, even though computers, servers, computer code and cookies can be used to accomplish wiretaps under the ECPA, only entities that intercept communications they are legally required to leave alone will face liability under the ECPA. *See* footnote 10, *supra.*

PointRoll neglects the other side, the privacy piracy side, of this slope that is actually slippery. Congress updated the Wiretap Act with the ECPA to protect privacy, including through civil actions, in a new technological age. *See* ECPA, P.L. 99-508. Legislative History at 5 ("Privacy cannot be left to depend solely on physical protection, or it will gradually erode as technology advances. Congress must act to protect the privacy of our citizens.")

B. COUNT II – THE COMPLAINT STATES A CLAIM UNDER THE STORED COMMUNICATIONS ACT

"[T]he Stored Communications Act protects individuals' privacy and proprietary interests." *Theofel v. Farey-Jones*, 359 F.3d 1066, 1072-73 (9th Cir. 2004). It provides a cause of action against "whoever (1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system. . . ." 18 U.S.C. § 2701(a). The "sort of trespasses to which the [ECPA] applies are those in which the trespasser gains access to information . . . which he is not entitled to see." *Therapeutic Research Faculty v. NBTY, Inc.*, 488 F.Supp.2d 991, 997 (E.D. Cal. 2007).

1. Browser-Managed Files on Computer and Mobile Devices are "Facilities" Under the SCA

PointRoll argues that the CAC fails to allege that it accessed a "facility." When PointRoll stores a third-party tracking cookie improperly without authorization and in spite of users' protection to block the deposit of such cookies, information about the user's activity is captured by these browser-managed files and ultimately transmitted to PointRoll. Therefore, PointRoll accesses "a facility through which an electronic communication service is provided," *i.e.*, Plaintiffs' browser-managed files on their computing devices. CAC ¶ 217-18.

The SCA does not define "facility," but Black's Law Dictionary defines "facilities" as that "which promotes the ease of any action, operations, transaction or course of conduct. The term denotes inanimate means rather than human agencies." Black's Law Dictionary p. 705 (4th Ed. 1951). "Congress intended the term to include the physical equipment used to facilitate electronic communications." *Council on Am.-Islamic Relations Action Network, Inc. v. Gaubatz*, 793 F. Supp. 2d 311, 334 (D.D.C. 2011). Plaintiffs allege a system involving numerous physical means of communication, including the user's hardware and browser-managed files. PointRoll stores an unauthorized cookie, and then obtains information from the user's browser-managed files. *See* CAC ¶¶ 27-48, 68-78, 127-145.

PointRoll also asserts that "mobile computers or products using the Apple operating system such as the iPhone or iPad have been held not to be 'facilities' under the SCA." D. Br. 16. Plaintiffs' browser-managed files are the facilities at issue through which an "electronic communication service" ("ECS")[18] is provided, e.g., internet service.[19] The computers and mobile phones on which the browser-managed files are stored by PointRoll are themselves "facilities," and therefore, contrary to PointRoll's assertion, the browser-managed files themselves must also be "facilities" under the SCA. *See Cousineau v. Microsoft Corp.*, No. C11-

[18] An ECS is "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15).

[19] PointRoll's cited cases inappositely apply the facts to § 2702, which prohibits ECS providers from knowingly disclosing contents of communications, and the courts found those Defendants were not themselves ECS providers. *In re Michaels Stores Pin Pad Litig.*, 830 F. Supp. 2d 518 (N.D. Ill. 2011) (credit card information stolen *from* Michaels and allegations Michaels itself was the ECS); *Dyer v. Nw. Airlines Corps.*, 334 F. Supp. 2d 1196 (D.N.D. 2004) (airline disclosed information provided by customers); *In re JetBlue Airways Corp. Privacy Litig.*, 379 F. Supp. 2d 299 (E.D.N.Y. 2005) (same). *Crowley v. CyberSource Corp.*, 166 F. Supp. 2d 1263 (N.D. Cal. 2001) involved both § 2701 & 2702 claims, but the facts were only that Amazon improperly shared information sent to it with a third party. Plaintiffs' claims are only under the quite different § 2701.

1438-JCC, slip op. at 10-11 (W.D. Wash. June 22, 2012) (See Ex. A attached hereto) ("Congress chose a broad term—facility—where it intended the statute to cover a particular function, such as internet access, as opposed to a particular piece of equipment providing that access, such as a router, laptop or smart phone. As technology evolves, identifying a smart phone as a facility through which an ECS is provided is not as 'strained' as it once may have seemed.").[20] Holding that a computer is a "facility," the *Cousineau* court noted: "While earlier stages of technological development may have required large facilities for data storage, the draw of mobile devices is that their smaller storage space enables communication and information access regardless of the user's location." *Id.* at 11.[21]

Discovery will allow Plaintiffs to further demonstrate that these physical means of communication constitute a "facility." *Gaubatz*, 793 F. Supp. 2d at 336 (denying dismissal because argument that plaintiffs' office computers are not a "facility" required "further development of the factual record"); *see also Cousineau*, NO. C11-1438-JCC, slip op. at 12.

2. PointRoll Accessed Information in "Electronic Storage"

PointRoll contends that Plaintiffs' SCA claim fails because it does not show PointRoll accessed anything in "electronic storage." The statute defines "electronic storage" as "(A) any

[20] *See also Chance*, 165 F. Supp. 2d 1153, 1161 (W.D. Wash. 2001) (SCA's definition of "facilities" includes PCs); *In re Intuit Privacy Litig.*, 138 F. Supp. 2d 1272, 1275 n.3 (C.D. Cal. 2001) ("The court notes, however, that Section 2701 does not require that Plaintiffs' computers be 'communication service providers' only that they be a **facility** through which an electronic communication service is provided.") (emphasis in original); *Expert Janitorial, LLC v. Williams*, No. 3:09-CV-283, 2010 WL 908740, at *5 (E.D. Tenn. Mar. 12, 2010) (citing *In re Intuit* and holding that "plaintiff's computers on which the data was stored may constitute 'facilities' under the SCA").

[21] Other cases PointRoll cites, *Garcia v. City of Laredo*, 702 F.3d 788 (5th Cir. 2012), and *Freedom Banc Mortgage Servs., Inc. v. O'Harra*, No. 2:11-CV-01073, 2012 WL 3862209 (S.D. Ohio Sept. 5, 2012), are distinguishable because Plaintiffs' allegations relate to files stored by PointRoll in Plaintiffs' browser-managed files, not from files stored permanently by owners on their hard drive. Moreover, *Garcia* is summary judgment, not a motion to dismiss, case. *Garcia*, 702 F.3d at 790.

temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof…." 18 U.S.C. § 2510(17). The SCA simply requires Plaintiffs to plead facts suggesting that data PointRoll accessed without authorization was temporarily stored pending delivery to an intended recipient. Plaintiffs have pled precisely that. *See* CAC ¶ 218. Plaintiffs allege extensive factual details explaining how PointRoll carried this out, *see* CAC ¶¶ ¶¶ 27-48, 68-78, 127-145, and how what was accessed was stored, *see* CAC ¶¶ 45-46, 130-134. Plaintiffs have met their burden of *pleading* facts that at a minimum "suggest" (*Phillips*, 515 F.3d at 233) that PointRoll accessed Plaintiffs' data while it was in "electronic storage."[22]

If the accessed files are stored for future use, as PointRoll stores its cookies in users' browser-managed files, they are stored in a "facility through which an electronic communication service is provided." 18 U.S.C. § 2701(a). Only PointRoll can store the cookies at issue in the browser through which the ECS is provided, as Plaintiffs were not even aware of their unauthorized placement and storage within their browser. So, the browser-managed files storing the cookies, in the "facilities" Plaintiffs alleged were accessed without authorization (CAC ¶ 217), are within the SCA's "electronic storage" definition. *See In re Intuit Privacy Litig.*, 138 F.Supp.2d at 1277 ("Plaintiffs have alleged that Defendant accessed data contained in 'cookies' that it placed in Plaintiffs' computers' electronic storage. The court concludes that this allegation satisfies the liberal requirements of Rule 8(a)(2)."); *see also Cousineau*, No. C11-1438-JCC, slip

[22] In light of the above, PointRoll's reliance on *In re DoubleClick* is misplaced. D. Br. 18. The plaintiff in *DoubleClick* alleged that the data files (cookies) at issue were *permanently* stored on their hard drives, leading the court to conclude, as a matter of law, that the defendants could not have accessed information in temporary "electronic storage." *In re DoubleClick*, 154 F. Supp. 2d at 512. The same is true of *In re Toys R Us, Inc., Privacy Litig.*, No. 00-CV-2746, 2001 WL 34517252, at *3-4 (N.D. Cal. Oct. 9, 2001), which relies heavily on *DoubleClick*. Here, Plaintiffs specifically allege that the cookies were temporarily stored by PointRoll when PointRoll accessed them without permission.

op. at 12 ("The language Congress chose, however, does not require only one point of ECS provision.").

C. COUNT III – PLAINTIFFS HAVE STATED A CLAIM UNDER THE COMPUTER FRAUD AND ABUSE ACT

PointRoll initially contends that Plaintiffs cannot state a claim under the CFAA because "[c]ookies are merely a few bytes of non-malicious code that are necessary to support intended browser functionality, and no court has found a legally cognizable injury from setting Internet cookies." D. Br. 8. Plaintiffs, however, have alleged much more than the mere placement of "necessary" cookies. Specifically showing how cookies facilitate tracking (*see, e.g.*, CAC ¶¶ 38-39, 78, 128-134), Plaintiffs allege "a scheme by which Defendants were bypassing the privacy settings of tens of millions of people who use Apple's Safari web browser to use the Internet" and that Defendants "exploited" an exception to Apple's privacy protection technology by "adding code to ads that tricked Safari into believing the exception had been satisfied." CAC ¶¶ 76-77; *see also* CAC ¶¶ 130-132 (detailing this deception). One of the cookies PointRoll then inserted surreptitiously, called "PRID," is a unique cookie designed to track persons across every website where PointRoll places ads. *Id.* at ¶ 134.

The cases PointRoll cites do not say that cookies are "merely a few bytes of non-malicious code" and do not preclude Plaintiffs' claim under the CFAA. For example, in *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040 (N.D. Cal. 2012) both plaintiff classes "voluntarily installed" the software that resulted in the alleged violation. *In re iPhone Application,* 844 F. Supp. 2d at 1066, 1068. To the contrary, Plaintiffs allege that PointRoll created an "invisible and fraudulent form submission" unbeknown to users. CAC ¶ 132. Not precluding claims concerning cookies, the court in *Specific Media*, 2011 WL 1661532, held that

the threat of re-activating previously deleted cookies "is potentially a threat of imminent harm" but that "it is not clear that Plaintiffs have even alleged this." *Id.* at *4.

PointRoll's red herring argument that "[t]he CFAA is primarily a criminal statute" (D. Br. 8) ignores Section 1030(g)'s plain language providing a civil remedy for "[a]ny person who suffers damage or loss by reason of a violation of this section." 18 U.S.C. § 1030(g). PointRoll's irrelevant quote from *Del Vecchio v. Amazon.com, Inc.*, No. C11-366 RSL, 2012 WL 1997697 (W.D. Wash. June 1, 2012), about cookies being "minute in size" and not "affecting the performance of modern computers" (D. Br 8) gains PointRoll nothing. The *Del Vecchio* court was addressing a claim that cookies "slowed down [plaintiffs'] Internet connection." *Del Vecchio*, 2012 WL 1997697 at *5. Plaintiffs here allege PointRoll's cookies permitted PointRoll's illicit tracking. CAC ¶¶ 127-135, 138.

1. Plaintiffs Have Alleged Sufficient Damage or Loss

The CFAA provides a civil remedy for "[a]ny person who suffers damage or loss by reason of a violation of this section." 18 U.S.C. § 1030(g). The statute defines "damage" as "any impairment to the integrity or availability of data, a program, a system, or information." 18 U.S.C. § 1030(e)(8). "Loss" is separately defined as "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system or information to its condition prior to the offense, and any other revenue lost, cost incurred, or other consequential damages incurred because of interruption of service." 18 U.S.C. § 1030(e)(11).

PointRoll created an "invisible and fraudulent form submission" designed to "evade[] Safari's default request for its cookies" (CAC ¶ 132), impairing Plaintiffs' browser default

system setting. PointRoll's resulting acquisition of user information is statutory "damage" because Defendant's seizure and use of that information impairs the integrity of that information.

PointRoll contends that Plaintiffs have not alleged any facts that they have suffered a $5,000 economic loss. D. Br. 10-11. The CFAA creates a civil penalty for anyone who "knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and ... furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period." 18 U.S.C. §1030(a)(4). Plaintiffs allege that Defendants knowingly and intentionally accessed protected computers, either without authorization or in excess thereof, and obtained something of value, namely third-party cookie data and PII. CAC ¶¶ 49-67. "Because [plaintiff] alleges that [defendant] obtained something of value beyond solely the use of the computer, the $5,000 requirement…is inapposite. Accordingly, the Court rejects [defendant]'s contention that [plaintiff]'s CFAA claim is subject to dismissal for failure to properly allege damages." *Oracle America*, 2012 WL 6019580, at *4.

Plaintiffs in any event do allege that the data PointRoll obtained is worth far more than $5,000. CAC ¶¶ 49-67. Plaintiffs specifically allege that the cash value of this personal information has recently been quantified as high as $4.20 per year for contact information, $3.00 per year for demographic information and $52.00 per year for web browsing histories. *Id.* ¶ 56.[23]

VI. CONCLUSION

PointRoll's Motion to Dismiss should be denied on all Counts.

[23] PointRoll relies on *In re Doubleclick*, 154 F. Supp. 2d at 524-26 for the argument that Plaintiffs cannot aggregate losses across the putative class. D. Br. at 11. The *In re Doubleclick* court concluded that the CFAA "only allows aggregation of damage over victims and time for a single act." *Id.* at 524. PointRoll's intentional circumvention of Safari (CAC ¶¶ 130-143) constitutes a "single act" for this purpose.

Dated: March 29, 2013

Respectfully submitted,

KEEFE BARTELS, LLC

/s/ Stephen G. Grygiel
Stephen G. Grygiel (Del Bar No. 4944)
John E. Keefe, Jr.
Jennifer L. Harwood
170 Monmouth St.
Red Bank, NJ 07701
Tel: 732-224-9400
sgrygiel@keefebartels.com

Executive Committee Member

STRANGE & CARPENTER

/s/ Brian Russell Strange
Brian Russell Strange
Keith Butler
David Holop
12100 Wilshire Boulevard, Suite 1900
Los Angeles, CA 90025
Tel: 310-207-5055
lacounsel@earthlink.net

Executive Committee Member

BARTIMUS, FRICKLETON, ROBERTSON & GORNY, P.C.

/s/ James P. Frickleton
James P. Frickleton
Mary D. Winter
Stephen M. Gorny
Edward D. Robertston, Jr.
11150 Overbrook Road, Suite 200
Leawood, KS 66211
Tel: 913-266-2300
jimf@bflawfirm.com

Executive Committee Member

STEWARTS LAW US LLP

/s/ Ralph N. Sianni
Ralph N. Sianni (Del Bar No. 4151)
Michele S. Carino (Del Bar. No. 5576)
Lydia E. York (Del Bar No. 5584)
I.M. Pei Building
1105 North Market Street, Suite 2000
Wilmington, DE 19801
Tel: 302-298-1200
rsianni@stewartslaw.com

Plaintiffs' Steering Committee Member and Liaison Counsel

EICHEN, CRUTCHLOW, ZASLOW & MCELROY LLP

/s/ Barry Eichen
Barry R. Eichen
40 Ethel Road
Edison, NJ 08817
Tel: 732-777-0100
beichen@njadvocates.com

Plaintiffs' Steering Committee Member

SEEGER WEISS LLP

/s/ Jonathan Shub
Jonathan Shub
1515 Market Street, Suite 1380
Philadelphia, PA 19102
Tel: 215-564-2300
jshub@seegerweiss.com

Counsel for Plaintiff Lynne Krause and Plaintiffs' Steering Committee Member

MURPHY P.A.

/s/ William H. Murphy, Jr.
William H. Murphy, Jr.
One South Street, Suite 2300
Baltimore, MD 21202
Tel: 410-539-6500
billy.murphy@murphypa.com

Plaintiffs' Steering Committee Member

BARNES & ASSOCIATES

/s/ Jay Barnes
Jay Barnes
219 East Dunklin Street
Jefferson City, MO 65101
Tel: 573-634-8884
Jaybarnes5@gmail.com

Plaintiffs' Steering Committee Member

BRYANT LAW CENTER, PSC

/s/ Mark Bryant
Mark Bryant
601 Washington Street
P.O. Box 1876
Paducah, KY 42002-1876
Tel: 270-442-1422
mark.bryant@bryantpsc.com

Counsel for Plaintiff William G. Gourley and Plaintiffs' Steering Committee Member